PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10	A1	(11) Numéro de publication internationale: **WO 99/18546**
		(43) Date de publication internationale: 15 avril 1999 (15.04.99)

(21) Numéro de la demande internationale: PCT/FR98/02104

(22) Date de dépôt international: 1er octobre 1998 (01.10.98)

(30) Données relatives à la priorité:
08/942,904 2 octobre 1997 (02.10.97) US

(71) Déposant: ACTIVCARD [FR/FR]; 24–28, avenue du Général de Gaulle, F–92150 Suresnes (FR).

(72) Inventeur: AUDEBERT, Yves; 15–433 Kennedy Road, Los Gatos, CA 95032 (US).

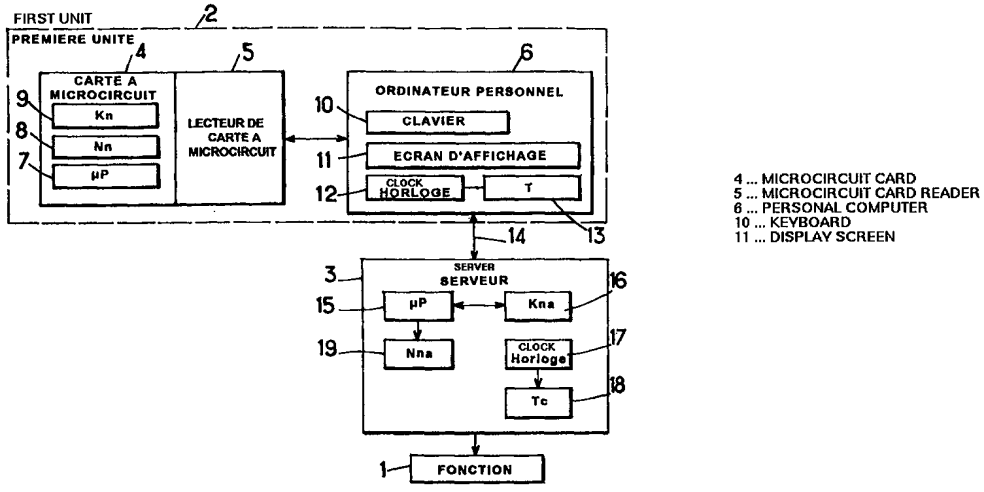
(74) Mandataire: CABINET DE BOISSE ET COLAS; 37, avenue Franklin D. Roosevelt, F–75008 Paris (FR).

(81) Etats désignés: CA, JP, SG, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: AUTHENTICATING SYSTEM WITH MICROCIRCUIT CARD

(54) Titre: SYSTEME D'AUTHENTIFICATION A CARTE A MICROCIRCUIT



(57) Abstract

The invention concerns a system comprising a first authentication unit (2) customised for a user and a verification unit (3) controlling access to a function (1). The first and second units comprise each means (13, 18) generating a dynamic variable (T, Ta) jointly, but independently, and means (7, 15) for working out a password (A, Aa) a function of the dynamic variable. The two passwords are compared in the second unit (3). The first unit comprises a microcircuit card (4) and a card reader (5). The means (12, 13) for generating the dynamic variable (T) and the means (7) for working out the password (A) in the first unit (2) are arranged respectively outside and inside the card (4). The card reader (5) transmits the dynamic variable (T) to said computing means (7) in the card.

(57) Abrégé

Le système comprend une première unité d'authentification (2) personnalisée pour un utilisateur et une unité de vérification (3) commandant l'accès à une fonction (1). Les première et deuxième unités comprennent chacune des moyens (13, 18) pour générer une variable dynamique (T, Ta) de concert, mais de manière indépendante, et des moyens (7, 15) pour calculer un mot de passe (A, Aa) fonction de ladite variable dynamique. Les deux mots de passe sont comparés dans la seconde unité (3). La première unité comprend une carte à microcircuit (4) et un lecteur de carte (5). Les moyens (12, 13) pour engendrer la variable dynamique (T) et les moyens (7) pour calculer le mot de passe (A) dans la première unité (2) sont disposés respectivement à l'extérieur et à l'intérieur de la carte (4). Le lecteur (5) de carte transmet la variable dynamique (T) auxdits moyens de calcul (7) dans la carte.

Système d'authentification à carte à microcircuit.

La présente invention est relative à un système électronique d'authentification d'individus et/ou de messages, en particulier pour contrôler l'accès d'un utilisateur à une fonction, permettant à un utilisateur d'obtenir conditionnellement un service ou une autre prestation devant être fourni par une unité de service spécialisé associée au système en question.

Plus particulièrement, l'invention concerne un système de contrôle d'accès à ou d'authentification de messages dans un ordinateur ou, plus généralement, un réseau informatique, dont l'utilisation est réservée à des personnes s'étant dûment légitimées. De tels réseaux peuvent servir par exemple à assurer toutes sortes de services impliquant une transaction, le plus souvent à contrepartie économique, telle que le télé-achat, la télévision à péage, la banque à domicile, les jeux télévisés interactifs, ou également le facsimile confidentiel, etc.

Le brevet U.S. 4,720,860 décrit un système d'authentification dans lequel, pour engendrer des mots de passe, on utilise une variable statique et une variable dynamique. Dans ce brevet, au début d'une procédure de demande d'accès, l'utilisateur doit entrer un code fixe dans une unité d'authentification ("token") chaque fois qu'une transaction doit être réalisée. Le code fixe est une variable statique. Une seconde variable est également engendrée dans l'unité d'authentification, et celle-ci varie de façon dynamique en fonction du temps, en particulier en fonction de l'instant auquel le code fixe est introduit dans l'unité d'authentification par l'utilisateur. Les deux variables, dont l'une est statique et l'autre dynamique, sont alors utilisées comme paramètres d'entrée d'un algorithme secret de chiffrement servant à engendrer un mot de passe dans l'unité d'authentification. Ce mot de passe est affiché sur l'unité d'authentification et l'utilisateur est invité à le transférer dans un serveur de vérification. Le code fixe est également transféré au serveur qui, en utilisant le même algorithme de chiffrement et une variable dynamique ayant

en principe la même valeur que celle utilisée dans l'unité d'authentification, calcule également le mot de passe. Ce dernier est comparé au mot de passe transmis au serveur par l'utilisateur et, s'il y a concordance, une autorisation d'accès à la fonction peut être délivrée. Ce système de contrôle d'accès emploie donc une variable statique à l'aide de laquelle l'algorithme de chiffrement calcule le mot de passe tout en utilisant également la variable dynamique.

Des systèmes d'authentification utilisant une variable dynamique fonction du temps pour engendrer des mots de passe sont également décrits dans les brevets U.S. 3,806,874, 4,601,011, 4,800,590.

Cette variable dynamique fonction du temps produite indépendamment dans l'unité d'authentification et dans le serveur, et les horloges de ces deux dispositifs utilisés pour engendrer la variable dynamique de part et d'autre, doivent être synchronisés avec une précision donnée.

La présente invention a pour but de fournir un système d'authentification offrant une meilleure sécurité contre les fraudes. Un autre but de l'invention est de fournir un système d'authentification fournissant des mots de passe dynamiques, en particulier des mots de passe dynamiques fonctions du temps, tout en utilisant au moins partiellement des moyens matériels conventionnels.

A cet effet, la présente invention a pour objet un système d'authentification pour contrôler l'accès d'au moins un utilisateur à une fonction, ledit système comprenant au moins une première unité personnalisée pour ledit utilisateur et au moins une seconde unité de vérification commandant l'accès à ladite fonction,

- ladite première unité comprenant :

- des premiers moyens générateurs pour engendrer au moins une variable dynamique ;

- des premiers moyens de calcul pour engendrer un premier mot de passe à l'aide d'au moins un premier algorithme de chiffrement utilisant des paramètres d'entrée fonction de ladite variable dynamique ; et

- des moyens pour transmettre ledit premier mot de passe à ladite seconde unité ;

• ladite seconde unité comprenant :

- des seconds moyens générateurs pour, en réponse à une demande d'accès faite à l'aide d'une déterminée desdites premières unités, engendrer au moins une variable dynamique assignée à cette première unité déterminée;

- des seconds moyens de calcul pour engendrer un second mot de passe à l'aide d'au moins un second algorithme de chiffrement utilisant des paramètres d'entrée fonction de ladite variable dynamique engendrée dans ladite seconde unité ;

- des moyens pour comparer lesdits premier et second mots de passe ; et

- des moyens pour, s'il y a une cohérence prédéterminée entre lesdits mots de passe, délivrer une autorisation d'accès à ladite fonction ;

• lesdits premier et second moyens générateurs prévus respectivement dans lesdites première et seconde unités engendrant ladite première variable dynamique de ladite première unité et ladite variable dynamique de ladite seconde unité de concert, mais de façon indépendante ;

• caractérisé en ce que

- ladite première unité comprend une carte à microcircuit comprenant les premiers moyens de calcul et un lecteur de carte et,

- lesdits moyens pour produire ladite variable dynamique de ladite première unité sont disposés à l'extérieur de ladite carte et ladite variable dynamique pour ladite première unité est transmise par ledit lecteur de carte auxdits premiers moyens de calcul dans ladite carte.

De préférence, ladite variable dynamique de chacune desdites première et seconde unités varie en fonction du temps.

Le système suivant l'invention combine les avantages de cartes telles que des cartes à microcircuits qui offrent un degré très élevé de sécurité en ce qui concerne le chiffrement de données mais ne possèdent pas de source d'énergie électrique propre, avec ceux de systèmes d'authentification fournissant des mots de passe dynamiques fonctions du temps.

D'autres caractéristiques et avantages de l'invention énumérés dans les sous-revendications ressortiront de la description qui va suivre donnée uniquement à titre d'exemple et faite en se référant aux dessins annexés sur lesquels :

La figure 1 est un schéma général d'un système d'authentification selon un premier mode de réalisation de l'invention ;

La figure 2 est un organigramme illustrant le principe de déroulement des opérations dans le système suivant l'invention, lorsqu'une demande d'accès est traitée ;

La figure 3 est un organigramme du mode de calcul d'une clé de chiffrement utilisée dans le calcul du mot de passe ;

La figure 4 montre une variante de réalisation des opérations représentées à la figure 2 ;

La figure 5 est un organigramme illustrant les opérations de calcul de mot de passe au moyen d'une version simplifiée du premier mode de réalisation représenté à la figure 1 ; et

La figure 6 est un schéma-bloc illustrant un second mode de réalisation de l'invention.

Sur la figure 1, on a représenté un schéma très simplifié d'un système d'authentification selon un premier mode de réalisation de l'invention.

Le système est supposé donner un accès conditionnel à une fonction qui est symbolisée par le rectangle 1 sur la figure 1. Le terme "fonction" doit être pris dans une acception très large. Il désigne toute fonction à laquelle l'accès est conditionné par une autorisation faisant intervenir une authentification impliquant une vérification du terminal à l'aide duquel la demande est formulée, et de préférence également une identification de la personne demandant l'accès à la fonction pour savoir si sa demande est légitime.

La fonction peut être de toute nature, par exemple une fonction d'accès à un local, à un réseau informatique ou à un ordinateur, à une transaction d'ordre pécuniaire (télé-achat, banque à domicile, jeu télévisé interactif,

télévision à péage), etc. La fonction peut impliquer également l'authentification de messages.

On voit sur le premier mode de réalisation représenté à la figure 1 que le système suivant l'invention comprend au moins une première unité d'authentification 2 et au moins une seconde unité de vérification 3. On notera que le système d'authentification suivant l'invention peut comporter un grand nombre de premières unités et une ou plusieurs secondes unités, mais en tout cas en un nombre de secondes unités nettement plus faible que celui des premières unités. Les nombres d'unités 2 et 3 ne sont donc nullement limitatifs de l'invention.

La première unité 2 comprend une carte à microcircuit 4, un lecteur 5 de carte à microcircuit et un calculateur 6 tel qu'un ordinateur personnel (PC) auquel le lecteur 5 de carte est connecté par une interface appropriée telle qu'un port RS-232 ou un port parallèle, un clavier ou une interface PCMIA.

La carte à microcircuit 4 comprend un microcontrôleur 7 convenablement programmé pour exécuter un algorithme cryptographique ALGO, ainsi que la mémoire ROM habituelle. Elle comporte également une mémoire programmable, telle qu'une EEPROM, représentée à la figure 1 par un registre 8 pour stocker le contenu Nn d'un compteur d'événements et par un registre 9 pour stocker une clé dynamique secrète Kn.

Le calculateur 6 comprend un clavier 10 destiné à permettre l'introduction de données, telles que par exemple le numéro d'identification personnel PIN de l'utilisateur de la carte à microcircuit 4. Il comprend également un écran d'affichage 11, et une horloge pour incrémenter un compteur 13 qui fournit une variable dynamique T représentant le temps. Le calculateur 6 comprend également le microprocesseur, les mémoires, les interfaces,..... habituels qui n'ont pas été représentés sur le dessin.

La seconde unité 3, dénommée ci-après le serveur, communique avec le calculateur ou ordinateur 6 par la liaison 14. Cette communication peut être assurée à courte distance ou longue distance par tout moyen approprié. Les données transmises sur cette liaison comprennent en particulier le mot de

passe devant être vérifié dans le serveur 3 et éventuellement des données à authentifier et traiter par le serveur.

Le serveur 3 comprend en particulier un processeur 15 capable de libérer conditionnellement les fonctions 1, visées par les demandes d'accès formulées par les différentes premières unités 2, ces fonctions pouvant être assurées à l'intérieur du serveur 3 ou à l'extérieur. Il est à noter que le serveur 3 coopère généralement avec un grand nombre de premières unités 2. Le serveur 5 comprend également une mémoire 16 pour stocker une clé dynamique secrète Kna pour chaque carte à microcircuit 4, une horloge 17 pour incrémenter un compteur 18 qui fournit une variable dynamique T_c représentant le temps, et une mémoire 19 pour stocker le contenu Nna d'un compteur d'événements pour chaque carte à microcircuit 4.

La figure 2 représente un organigramme simplifié des diverses opérations qui se déroulent lorsqu'une demande d'accès à une fonction est formulée par l'utilisateur d'une première unité 2. La figure 2 est divisée en deux parties, la partie à gauche du trait en pointillés L représentant les opérations exécutées dans la première unité 2 et la partie à droite de ce trait montrant celles qui se déroulent dans le serveur 3.

La carte 4 est personnalisée de manière à être attribuée personnellement à un utilisateur donné. Elle porte un numéro d'identification public ("USER ID") et/ou ce nombre peut être enregistré dans celle-ci sous forme non chiffrée et attribué à cette carte au moment de son initialisation. Il peut également être formé par le nom de l'utilisateur ou toute autre information qui lui est spécifique.

Pour initier la procédure dans le serveur 3, le numéro d'identification public (USER ID) doit être d'abord communiqué au serveur 15. Cette opération peut être assurée de différentes manières. Le numéro d'identification public (USER ID) peut être transmis au serveur 3 par le calculateur 6, par exemple directement aussitôt que la carte 4 est introduite dans le lecteur 5, ou après qu'il ait été introduit au clavier 10 du calculateur 6 par l'utilisateur lui-même.

L'utilisateur doit également donner sa légitimation en tapant, en 20, son code d'identification personnel ou code PIN au clavier 10 du calculateur 6. Le

code introduit au clavier est vérifié en 21 dans la carte 4 par comparaison avec le code PIN stocké dans la mémoire de la carte 4. En cas de discordance, la demande d'accès est immédiatement refusée en 22 par la carte 4, l'utilisateur pouvant se voir allouer éventuellement plusieurs tentatives consécutives avant qu'un refus définitif lui soit opposé, si elles restent toutes infructueuses.

Si au contraire le code PIN introduit et le code PIN mémorisé concordent, le programme déclenche en 23 l'opération de calcul du mot de passe dans la carte 4.

Le calcul consiste en un chiffrement à l'aide d'un algorithme de chiffrement qui peut être secret ou public (bloc 25). Dans ce dernier cas, il peut s'agir d'un algorithme appelé DES (Data Encryption Standard) par les spécialistes de cette technique.

L'algorithme en question utilise des paramètres d'entrée fonction de variables dynamiques qui, dans le cas représenté, sont au nombre trois. Deux d'entre elles sont une variable Nn stockée dans le registre 8 de la carte 4 et qui représente le nombre de demandes d'accès effectué par la carte 4, et une variable T représentant le temps actuel et correspondant à la position du compteur 13 du calculateur 6. Lors de l'initialisation, ces variables peuvent être fixées à des valeurs initiales, NO et/ou TO respectivement, qui ne sont pas nécessairement égales à 0 et qui peuvent être secrètes ou non. De même, Nn et T peuvent varier selon des fonctions faisant intervenir des paramètres tels qu'entre autres le nombre de demandes d'accès, une fonction du nombre de demandes d'accès et le temps actuel respectivement.

Plus particulièrement, à la figure 2, une fois que l'utilisateur a été identifié par la première unité 2 au moyen de l'introduction du numéro d'identification personnel ou PIN par le clavier 10, le PC 6 lit le contenu Nn du compteur d'événements 8 dans la carte 4.

Chacune des variables Nn et T peut comporter 32 bits et être soumise préalablement à une opération de concaténation dans le calculateur 6, en 24, offrant ainsi un paramètre d'entrée ou "challenge" de 64 bits au total. L'opération effectuée en 24 peut, en variante, être constituée par tout traitement ou combinaison comme l'entrelaçage, le hachage, une opération

OU-EXCLUSIF ou ET, etc. effectué sur Nn et T. En d'autres termes, l'opération en 24 n'est pas limitée à ces diverses variantes, mais elle peut consister en toute opération exécutée dans le but de produire une sortie (par exemple sur 64 bits) par combinaison ou traitement de Nn et T selon l'une de virtuellement un nombre infini de possibilités.

Ce challenge est appliqué par le calculateur 6 à la carte à microcircuit 4 et est chiffré par l'algorithme ALGO en 25 au moyen de la clé de chiffrement Kn stockée dans le registre 9 de la carte à microcircuit 4. Un autre moyen de définir l'algorithme mis en œuvre en 25 consiste à dire que l'algorithme génère un mot de passe en fonction des valeurs actuelles de Nn, T et Kn ou que Kn est chiffré en fonction d'une clé comprenant une valeur engendrée par concaténation de Nn et T en 24.

Le chiffrement effectué en 25 dans la carte 4 génère un mot de passe A en 26 et provoque l'incrémentation d'une unité par le calculateur 6, en 27, de la position du registre 8 de demande d'accès de la carte 4 qui stocke Nn. Le nombre incrémenté Nn+1 est stocké dans le registre 8 et soumis à une opération de calcul en 28 dans la carte 4 pour calculer la nouvelle valeur Kn+1 de la troisième variable dynamique ou clé de chiffrement secrète. En variante, la sortie du bloc 27 pourrait commander l'incrémentation du registre 8 d'un autre nombre que le nombre 1, c'est-à-dire que l'incrémentation pourrait être de deux unités (ou tout autre nombre) à chaque fois. De même, le nombre d'unités d'incrémentation peut varier d'une demande d'accès à la suivante. Bien entendu, l'incrémentation doit alors être synchronisée avec celle mise en œuvre dans le serveur 3.

Un exemple des opérations pouvant être effectuées en 28 pour le calcul de cette nouvelle valeur est représenté à la figure 3. Ces opérations sont effectuées de concert aussi bien dans la carte à microcircuit 4 que dans le serveur 3. Tout d'abord, les valeurs Nn+1 et Kn sont soumises en 29 à une opération de combinaison logique, par exemple une combinaison OU-EXCLUSIF. La variable intermédiaire résultante Z est soumise à un chiffrement en 30 à l'aide d'un algorithme connu ou public qui peut être le même que celui utilisé en 25. Le chiffrement peut être effectué à l'aide d'une

clé de chiffrement qui est de préférence la valeur de la variable dynamique actuelle Kn, bien qu'une autre clé secrète Q (bloc 31) puisse également être utilisée.

Le résultat de l'opération de chiffrement en 30 est la nouvelle valeur Kn+1 de la clé de chiffrement qui va être utilisée lors de la prochaine demande d'accès. Cette valeur est mémorisée dans le registre 9.

Après obtention du mot de passe A qui est affiché sur l'écran 11 du calculateur 6 en 32, l'utilisateur est invité à le communiquer au serveur 3. Il est à noter que ce mot de passe peut être le résultat complet de l'opération de chiffrement en 25 (d'une longueur de 64 bits) ou bien seulement une partie de ce résultat, par exemple un mot de 32 bits. Cette communication (symbolisée par le trait en pointillés 33) peut se faire par exemple en tapant le mot sur le clavier 10 du calculateur 6. Cette communication peut également être réalisée automatiquement, par exemple par modem, et dans ce cas il n'est pas nécessaire que le mot de passe A soit présenté à l'utilisateur en 32.

Lors de l'introduction dans le serveur 3 du numéro d'identification public (USER ID), le programme du microprocesseur 15 exécute, de concert avec la première unité 2 et à l'aide de variables dynamiques engendrées indépendamment par rapport à la première unité 2, des opérations de calcul identiques à celles exécutées dans celle-ci. Ces opérations ont donc été indiquées sur la figure 2 par les mêmes références numériques suivies de la lettre "a". En réponse à la demande d'accès, par exemple à la transmission du numéro d'identification au serveur 3, les variables Kna et Nna sont extraites des mémoires 16 et 19 du serveur 3. Les mémoires 16 et 19 stockent les variables Kna et Nna de chaque carte 4 à microcircuit avec lesquelles le serveur est appelé à coopérer.

En réponse à la demande d'accès, la variable T_c est également extraite du compteur 18. Si les calculateurs 6 qui sont utilisés avec les cartes à microcircuit 4 n'ont pas été tous initialisés à la même valeur T0, le calculateur 6 doit être identifié par le serveur 3, par exemple au moment où le numéro USER ID est transmis au serveur 3. En réponse à cette identification, le microprocesseur 15 lit dans une mémoire la valeur initiale T0 de la variable T

pour ce calculateur et calcule à partir de T0 et de T_c une variable de temps Ta qui doit être égale à la variable de temps T dans le calculateur 6.

Par conséquent, le serveur 3 produit de son côté, et sans que les variables dynamiques produites dans la première unité 2 lui soient communiquées, un mot de passe Aa qui est comparé avec le mot de passe A transmis au serveur 3 par l'utilisateur. Si la carte à microcircuit 4 est authentique, les mots de passe A et Aa doivent être identiques ou du moins concorder selon des règles prédéterminées. Si le test en 34 aboutit à une réponse affirmative, la fonction 1 est libérée. Dans le cas contraire, l'accès sera refusé en 35.

Il est à noter qu'avec un système selon l'invention, des problèmes peuvent surgir lorsque l'une des variables dynamiques est le temps ou une fonction de celui-ci comme décrit ci-dessus, étant donné qu'une dérive des horloges utilisées à la fois dans les calculateurs 6 et dans le serveur 3 peut se produire. Une solution avantageuse à ce problème est décrite dans WO97/36263.

On constate donc que, selon le mode de réalisation décrit, le processus d'authentification de la première unité 2 conduisant à la libération de la fonction en 1 est réalisé à l'aide de trois variables dynamiques, dont l'une est la clé de chiffrement Kn (Kna) et dont les autres sont le nombre Nn (Nna) de demandes d'accès déjà effectuées et le temps T (Ta) (ou des nombres calculés suivant une fonction prédéterminée de ces variables).

La clé de chiffrement Kn (Kna) elle-même dérive d'une demande d'accès à l'autre et elle est dynamiquement variable en fonction de la valeur Nn (Nna) avec laquelle elle peut être combinée logiquement, puis chiffrée pour donner lieu à la clé de chiffrement Kn+1 (Kna+1) utilisée lors de la prochaine demande d'accès.

Suivant une variante de l'invention, on peut envisager un transfert de données de la première unité 2 au serveur 3 afin que les données puissent être traitées lors de l'accomplissement de la fonction 1, dans la mesure naturellement où l'autorisation a été donnée pour cela à la suite du test en 34.

L'utilisateur, en formulant sa demande d'accès, introduit en 36 les données dans la première unité 2 à l'aide de son clavier 10. Ces données sont combinées logiquement en 37 avec la valeur concaténée des deux variables Nn et T, le résultat étant utilisé comme paramètre d'entrée de la procédure de chiffrement effectuée en 25. En variante, les données peuvent également être combinées directement avec le résultat de l'opération de chiffrement en 25 ou bien les données peuvent constituer une autre clé pour l'algorithme en 25. L'aspect essentiel est que la sortie du bloc 25 soit une fonction des données à transférer.

Les données sont également transférées au serveur 3, par exemple au moyen du clavier 10 du calculateur 6 ou automatiquement par l'intermédiaire de la liaison 14.

Les données ainsi reçues en 36a dans le serveur 3 y sont traitées de la même façon que dans la première unité 2. Plus particulièrement, les données peuvent être combinées par une opération logique en 37a avec la valeur concaténée de Nna et Ta, le résultat étant utilisé comme paramètre d'entrée pour le processus de chiffrement en 25a. En variante, les données peuvent directement être combinées avec le résultat de l'opération de chiffrement en 25a ou bien les données peuvent constituer une autre clé pour l'algorithme en 25a. Les données sont aussi communiquées en clair au dispositif chargé d'exécuter la fonction 1.

Ainsi, l'authenticité des données peut être vérifiée par comparaison des mots de passe A et Aa qui sont tous deux des fonctions de la valeur représentant les données. La mise en œuvre de la fonction 1 recevra donc un refus s'il y a non concordance entre les données présentées des deux côtés.

Plusieurs autres modes de réalisation seront maintenant décrits, certains d'entre eux l'étant en faisant référence à des changements se produisant dans la première unité 2, mais on comprendra que ces mêmes changements s'appliquent également au serveur 3 car la première unité 2 et le serveur 3 doivent pouvoir engendrer des mots de passe identiques ou concordant A, Aa.

En variante, la fonction 28 (représentée aux figures 2 et 3) peut varier en fonction de T. De même l'algorithme 30 peut être changé à chaque nouvelle dérivation de Kn. De façon similaire, l'algorithme utilisé en 25 peut être changé à chaque fois qu'un mot de passe est engendré. Par exemple, les modules 25, 25a et 30, 30a peuvent stocker plusieurs algorithmes utilisés distinctement au cours des différentes opérations de calcul des mots de passe. Des changements synchronisés doivent alors être réalisés dans le serveur 3 en ce qui concerne la fonction 28a, l'algorithme 30a et l'algorithme 25a.

De plus, la fonction 29 (figure 3) peut être différente d'une fonction OU-EXCLUSIF, telle qu'une opération ET ou toute autre opération logique. De plus, la fonction 29 n'est pas indispensable, Nn+1 pouvant directement être utilisé par l'algorithme 30 de façon à être chiffré par Kn et Q. De même, en variante, Q peut être soumis avec Nn+1 à une opération OU-EXCLUSIF en 29, Kn et Q étant utilisés comme clé de chiffrement pour le chiffrement de la sortie produite par l'opération logique en 29.

Une autre modification consiste à prévoir une porte ET entre les modules 26 et 27 de la figure 2, la sortie du module 26 constituant l'une des entrées de cette porte ET, l'autre entrée en étant formée par un signal provenant du serveur 3 et qui n'est engendré que si le module 26a engendre une sortie. De cette manière, le registre 8 dans la carte 4 et le registre 19 dans le serveur 3 seront incrémentés de façon synchrone. Il n'y aura alors aucune perte de synchronisation des valeurs Nn et Nna. Cependant, dans certaines applications de la présente invention, une telle communication en retour du serveur vers la carte peut ne pas être souhaitable.

Une autre variante consiste à stocker les données en 36 dans la mémoire de la carte à microcircuit 4. Par exemple, si la carte 4 est une carte bancaire, les données en 36 pourraient être la situation d'un compte bancaire, un numéro de compte, etc.

La dérivation de Kn selon les fonctions 28 et 28a peut également être exécutée comme suit. Kn peut être dérivé deux fois pour chaque calcul du mot de passe. On peut le faire par exemple avant et après le calcul du mot de

passe. Kn peut également être redérivé en parallèle avec le calcul du mot de passe. En d'autres termes, Kn peut être redérivé pendant le calcul d'un mot de passe, les sorties du module 25 et du module 25a étant alors directement utilisées comme entrées des modules 27 et 27a respectivement.

En variante, Nn et T peuvent être introduits directement dans le module de chiffrement 25. Les données peuvent également être combinées logiquement directement avec Nn et T, ou encore les données peuvent être scindées en deux parties combinées respectivement avec Nn ou T.

La figure 4 montre une variante du premier mode de réalisation qui simplifie le logiciel implanté dans l'ordinateur personnel PC et limite les échanges d'informations entre l'ordinateur personnel PC et la carte à microcircuit. Sur la figure 4, les mêmes références que sur la figure 2, mais augmentées du nombre 100, ont été utilisées pour désigner des éléments correspondants. Ce qui manque dans la carte à microcircuit 104 est le compteur d'horloge 113 stockant la variable de temps T. Toutes les autres fonctions mises en œuvre pour la génération du mot de passe sont implantées dans la carte à microcircuit 104.

Une fois que l'utilisateur a été identifié en 121 par la première unité 102 grâce à l'introduction du numéro d'identification personnel ou PIN dans le clavier, l'ordinateur personnel ou PC 106 envoie la variable T stockée dans le compteur 113 à la carte à microcircuit 104. En 124, Nn et la variable T sont concaténés ou traités d'une autre manière, comme décrit ci-dessus à propos de la figure 2, pour générer dans la carte 104 un paramètre d'entrée ou challenge de, par exemple, 64 bits. Ce challenge est chiffré par l'algorithme ALGO en 125 en utilisant la clé de chiffrement Kn stockée dans le registre 109.

Le chiffrement effectué en 125 génère en 126 le mot de passe A qui est formaté et affiché sur l'écran du PC 106 en 132. Ce mot de passe A est communiqué au serveur ou seconde unité 103 comme décrit en regard de la figure 2. Bien entendu, si l'ordinateur personnel 106 communique directement le mot de passe A à la seconde unité 103, par exemple par modem, il n'est pas nécessaire, d'afficher le mot de passe A pour l'utilisateur.

Le chiffrement effectué en 125 provoque également l'incrémentation en 127 de la valeur Nn, et la nouvelle valeur Nn+1 est stockée dans le registre 108 de la carte à microcircuit 104. L'incrémentation peut être une incrémentation d'une unité ou un autre type d'incrémentation comme décrit ci-dessus. Le nombre incrémenté Nn+1 est également soumis en 128 à une opération de calcul pour calculer une nouvelle valeur Kn+1 de la troisième variable dynamique ou clé de chiffrement secrète. Cette opération de calcul a également été décrite ci-dessus.

Une version simplifiée du premier mode de réalisation, représentée à la figure 5, peut consister à éliminer le compteur d'événements et la dérivation de clé, c'est-à-dire les variables dynamiques autres que T, la clé Kn étant statique. Sur la figure 5, les mêmes références que sur la figure 2, mais augmentées du nombre 200, ont été utilisées pour désigner les éléments correspondants. En dehors de la suppression du compteur d'événements et de la dérivation de clé, les différentes opérations représentées à la figure 5 sont semblables à celles des figures 2 et 4 et ne seront pas décrites en détail.

Le lecteur 5 de carte à microcircuit représenté dans le premier mode de réalisation des figures 1 à 5 est un lecteur passif de carte à microcircuit, c'est-à-dire qu'il transmet simplement les données entre la carte 4 à microcircuit et l'ordinateur personnel 6. En variante, le lecteur 5 de carte à microcircuit peut être un lecteur "intelligent" ou actif de carte à microcircuit et peut être portable. Le second mode de réalisation de l'invention, visant l'utilisation d'un tel lecteur "intelligent" de carte à microcircuit, est représenté à la figure 6.

Comme représenté à la figure 6, dans la première unité 302, le lecteur "intelligent" 305 de carte à microcircuit lit la carte à microcircuit 304 du premier mode de réalisation et est adapté pour être utilisé avec une seconde unité 303 qui peut être la même que la seconde unité 3, 103 ou 203. Le lecteur 305 de carte à microcircuit comprend un clavier 310, un écran d'affichage 311, un registre 313 et une horloge 312 correspondant au clavier 10, à l'écran d'affichage 11, au registre 13 et à l'horloge 12 et peut également comporter sa propre source d'énergie électrique, telle qu'une batterie 350. Un tel lecteur de

carte à microcircuit peut mettre en œuvre les fonctions décrites à la figure 2 pour le PC 306, ou aux figures 4 et 5 pour les PC 106 et 206 respectivement.

Comme indiqué ci-dessus, le lecteur 305 de carte à microcircuit peut être configuré pour fournir T, et la carte à microcircuit 304 peut être configurée pour mettre en œuvre les autres opérations de la première unité 302 comme décrit à propos des figures 4 et 5.

En variante, le lecteur 305 de carte à microcircuit peut être configuré pour mettre en œuvre les mêmes opérations que l'ordinateur personnel 6 de la figure 2 et la carte à microcircuit 304 peut être configurée pour mettre en œuvre les autres opérations de la première unité 302. En variante, comme décrit ci-dessus, la variable de temps T peut être fournie par un ordinateur personnel PC 306 au lecteur 305 de carte à microcircuit, supprimant ainsi la nécessité de l'horloge 312 dans le lecteur 305.

Une première unité telle que 2, 102, 202 ou 302 peut être implantée dans n'importe quel dispositif possédé par l'utilisateur tel qu'un assistant numérique personnel (PDA), un téléphone cellulaire ou autre type de récepteur téléphonique, pour autant qu'un tel dispositif est configuré du point de vue matériel et/ou logiciel pour lire une carte à microcircuit et mettre en œuvre les fonctions décrites à propos des figures 2, 4 ou 5.

La présente invention se distingue de la technique antérieure du fait que la variable dynamique T représentant le temps actuel n'est pas engendrée là où l'algorithme et les clés sont stockés et mis en œuvre. La technique antérieure décrit des modes de réalisation dans lesquels la génération d'un signal d'horloge est réalisée là où l'algorithme et les clés sont stockés. La présente invention est basée sur le fait qu'une variable fonction du temps est engendrée en dehors de la carte à microcircuit par un ordinateur personnel ou un lecteur "intelligent" de carte et transmise à la carte à microcircuit pour générer un mot de passe utilisant une clé stockée dans la carte à microcircuit. Cet agencement est avantageux car, sans qu'aucune source d'énergie permanente soit requise dans la carte, il combine les avantages des mécanismes de sécurité matériels et logiciels disponibles dans une carte à microcircuit avec ceux offerts par des mots de passe dynamiques fonction du

temps qui sont plus sûrs que des mots de passe statiques. Cet agencement est également avantageux car il permet d'utiliser des dispositifs électroniques répandus très largement tels que des ordinateurs personnels, des assistants numériques personnels, des téléphones cellulaires, etc..., qui ne sont généralement pas sécurisés, pour fournir, en combinaison avec une carte à microcircuit, un système d'authentification hautement sécurisé délivrant des mots de passe dynamiques fonction du temps.

Il va de soi pour les spécialistes de la technique que la présente invention n'est pas limitée à ce qui a été spécifiquement décrit ci-dessus et représenté et, en particulier, n'est pas limitée aux modes de réalisation décrits. Bien au contraire, d'autres modifications peuvent être faites sans sortir pour cela du cadre de l'invention. De plus, des variantes décrites séparément peuvent être combinées.

REVENDICATIONS

1. Système d'authentification pour contrôler l'accès d'au moins un utilisateur à une fonction, ledit système comprenant au moins une première unité (2 ; 102 ; 202 ; 302) personnalisée pour ledit utilisateur et au moins une seconde unité de vérification (3 ; 103 ; 203 ; 303) commandant l'accès à ladite fonction,

• ladite première unité (2 ; 102 ; 202 ; 302) comprenant :

- des premiers moyens générateurs (13 ; 113 ; 213 ; 313) pour engendrer au moins une variable dynamique (T) ;

- des premiers moyens de calcul (24, 25 ; 124, 125 ; 225) pour engendrer un premier mot de passe (A) à l'aide d'au moins un premier algorithme de chiffrement (ALGO) utilisant des paramètres d'entrée fonction de ladite variable dynamique (T) ; et

- des moyens (10 ; 33) pour transmettre ledit premier mot de passe à ladite seconde unité ;

• ladite seconde unité (3 ; 103 ; 203 ; 303) comprenant :

- des seconds moyens générateurs (18 ; 118 ; 218) pour, en réponse à une demande d'accès faite à l'aide d'une déterminée desdites premières unités, engendrer au moins une variable dynamique (Ta) assignée à cette première unité déterminée;

- des seconds moyens de calcul (24a, 25a ; 124a, 125a ; 225a) pour engendrer un second mot de passe (Aa) à l'aide d'au moins un second algorithme de chiffrement utilisant des paramètres d'entrée fonction de ladite variable dynamique (Ta) engendrée dans ladite seconde unité ;

- des moyens (34 ; 134 ; 234) pour comparer lesdits premier et second mots de passe (A, Aa) ; et

- des moyens (34 ; 134 ; 234) pour, s'il y a une cohérence prédéterminée entre lesdits mots de passe (A, Aa), délivrer une autorisation d'accès à ladite fonction (1) ;

• lesdits premiers et seconds moyens générateurs prévus respectivement dans lesdites première et seconde unités engendrant ladite première variable dynamique (T) de ladite première unité et ladite variable

dynamique (Ta) de ladite seconde unité de concert, mais de façon indépendante ;

• caractérisé en ce que

- ladite première unité comprend une carte à microcircuit (4 ; 104 ; 204 ; 304) comprenant les premiers moyens de calcul, et un lecteur de carte (5, 105 ; 205 ; 305) et,

- lesdits moyens (12, 13 ; 113 ; 213 ; 312, 313) pour produire ladite variable dynamique (T) de ladite première unité (2 ; 102 ; 202 ; 302) sont disposés à l'extérieur de ladite carte et ladite variable dynamique (T) pour ladite première unité est transmise par ledit lecteur de carte audit premier moyen de calcul dans ladite carte.

2. Système selon la revendication 1, caractérisé en ce que ladite variable dynamique (T, Ta) pour chacune desdites première et deuxième unités varie en fonction du temps.

3. Système selon la revendication 2, caractérisé en ce que l'un desdits paramètres d'entrée pour générer lesdits premier (A) et second (Aa) mots de passe est une clé de chiffrement (Kn, Kna ; K, Ka) utilisée dans lesdits premier et second algorithmes.

4. Système selon la revendication 3, caractérisé en ce que lesdites première (2 ; 102 ; 302) et seconde (3, 103 ; 303) unités respectivement comprennent des troisièmes (8 ; 108) et quatrièmes (19 ; 119) moyens générateurs pour produire au moins une seconde variable dynamique (Nn, Nna) conformément à une fonction impliquant un nombre de demandes d'accès effectuées par ladite première unité avant une demande d'accès en cours, lesdits premiers (24, 25 ; 124, 125) et seconds (24a, 25a ; 124a, 125a) moyens de calcul produisant respectivement lesdits premier (A) et second (Aa) mots de passe en fonction desdites première (T, Ta) et seconde (Nn, Nna) variables dynamiques.

5. Système selon la revendication 4, caractérisé en ce que lesdites première (2 ; 102 ; 302) et seconde (3, 103 ; 303) unités comprennent des cinquièmes (28 ; 128) et sixièmes (28a ; 128a) moyens générateurs pour produire au moins une troisième variable dynamique (Kn, Kna) suivant une

fonction impliquant l'une au moins desdites première et seconde variables dynamiques (T, Ta, Nn, Nna), lesdits premiers (24, 25 ; 124, 125) et seconds (24a, 25a ; 124a, 125a) moyens de calcul produisant respectivement lesdits premier (A) et second (Aa) mots de passe en fonction desdites première (T, Ta), seconde (Nn, Nna) et troisième (Kn, Kna) variables dynamiques.

6. Système selon la revendication 5, caractérisé en ce que lesdites première (2 ; 102 ; 302) et seconde (3 ; 103 ; 303) unités comprennent des troisièmes (24 ; 124) et quatrièmes (24a ; 124a) moyens de calcul respectivement pour produire une variable dynamique intermédiaire par combinaison logique desdites première (T, Ta) et seconde (Nn, Nna) variables dynamiques, lesdits premiers (25 ; 125) et seconds (25a ; 125a) moyens de calcul produisant lesdits premier (A) et second (Aa) mots de passe en fonction de ladite variable dynamique intermédiaire et de ladite troisième variable dynamique (Kn, Kna) respectivement.

7. Système selon la revendication 6, caractérisé en ce que lesdits troisièmes moyens de calcul (124) sont disposés dans ladite carte (104).

8. Système selon la revendication 6, caractérisé en ce que lesdits troisièmes moyens de calcul (24) sont disposés en dehors de ladite carte (4).

9. Système selon l'une quelconque des revendications 5 à 8, caractérisé en ce que ladite seconde variable dynamique (Nn, Nna) est ledit nombre de demandes d'accès effectuées par ladite première unité (2 ; 102 ; 302) préalablement à une demande d'accès en cours et ladite troisième variable dynamique (Kn, Kna) est une fonction de ladite seconde variable dynamique (Nn, Nna) et de la valeur précédente de ladite troisième variable dynamique.

10. Système selon l'une quelconque des revendications 5 à 9, caractérisé en ce que ladite troisième variable dynamique (Kn, Kna) est ladite clé de chiffrement.

11. Système selon l'une quelconque des revendications 2 à 10, caractérisé en ce que lesdits moyens (312, 313) pour produire ladite première variable dynamique (T) sont disposés dans ledit lecteur de carte (305).

12. Système selon l'une quelconque des revendications 2 à 10, caractérisé en ce que ladite première unité (2 ; 102 ; 202) comprend un ordinateur personnel (6 ; 106 ; 206) comprenant lesdits moyens (12, 13 ; 113 ; 213) pour générer ladite première variable dynamique (T) et des moyens de connexion audit lecteur de carte (5 ; 105 ; 205).

13. Système selon les revendications 11 ou 12, caractérisé en ce que lesdits moyens (12, 13 ; 113 ; 213 ; 312, 313) pour produire ladite première variable dynamique (T) comprennent une horloge (12 ; 312) et un compteur (13, 113 ; 213 ; 313).

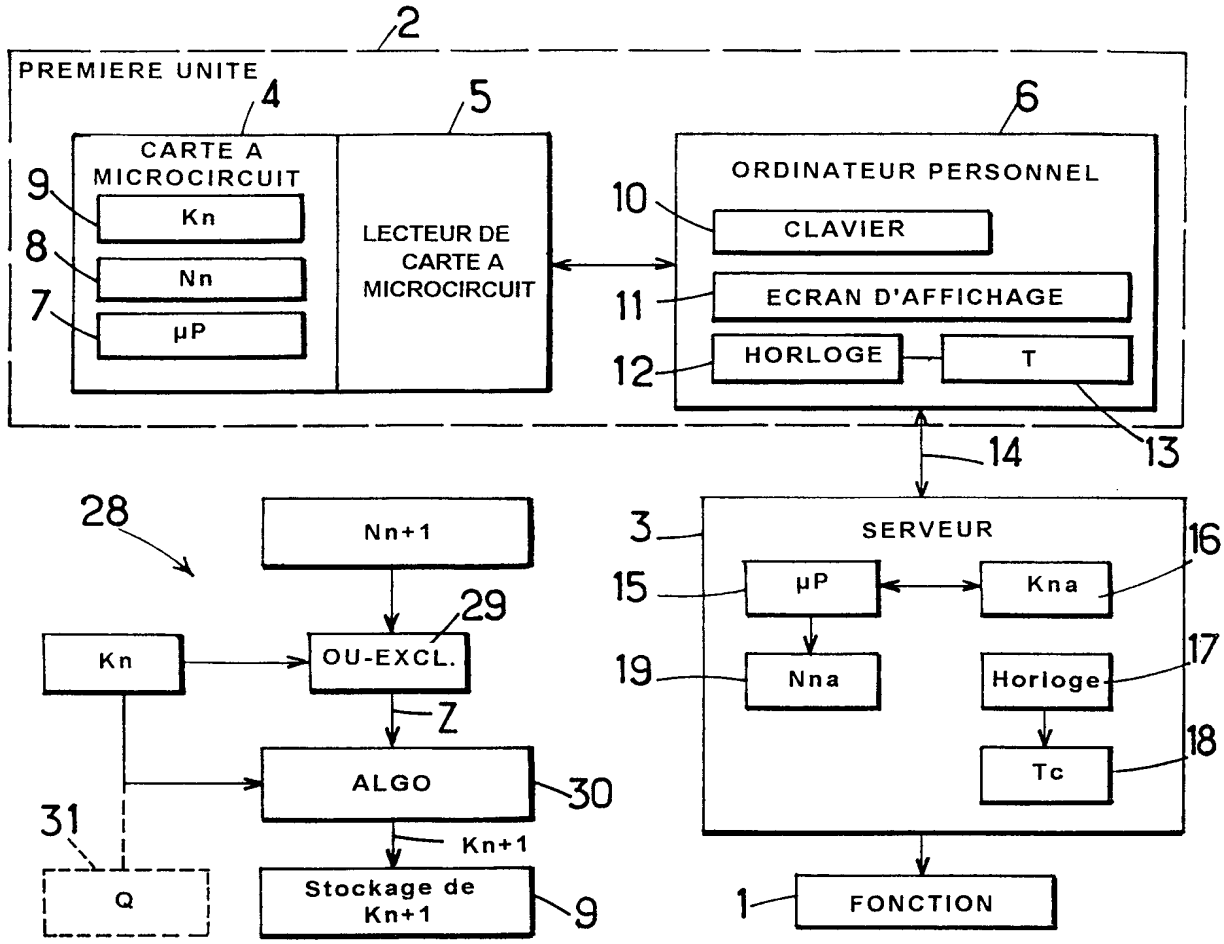
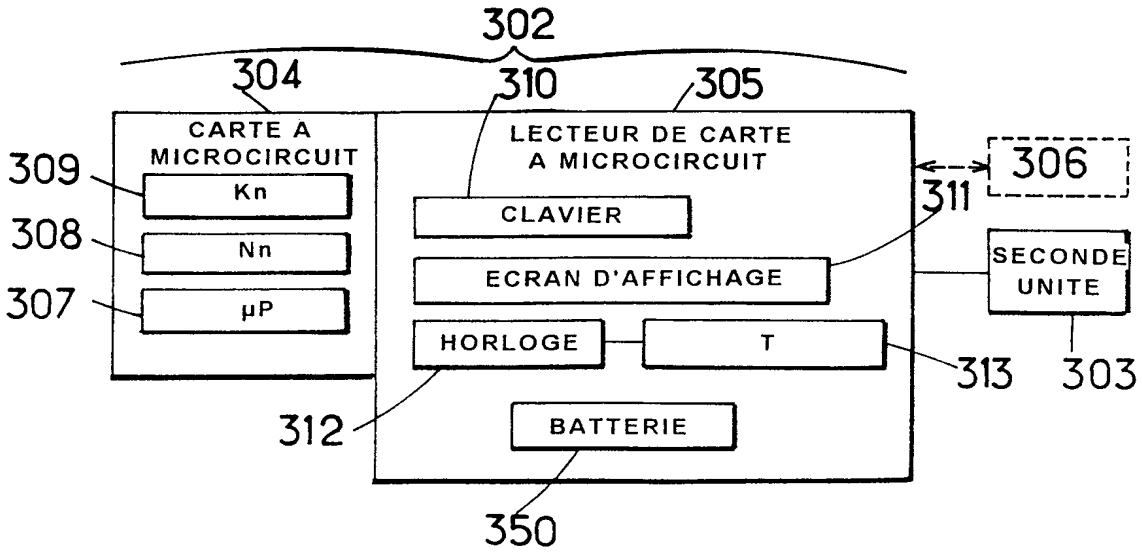


FIG.:3

FIG.:1

FIG.:6



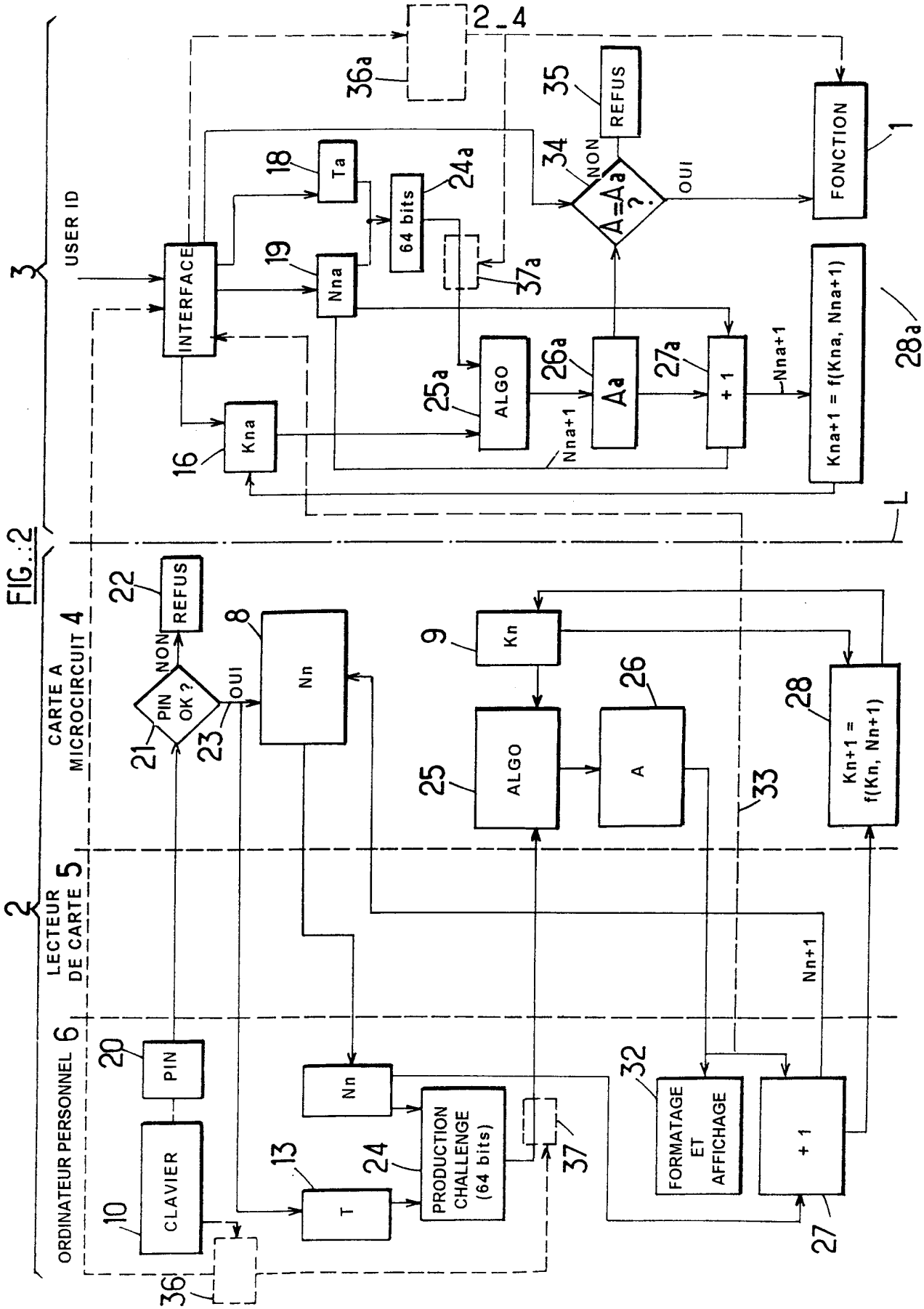

2
3
4
5
6
USER ID
INTERFACE
Ta
Nna
64 bits
Kna
ALGO
Aa
+ 1
A=Aa ?
NON
OUI
REFUS
FONCTION
Kna+1 = f(Kna, Nna+1)
Nna+1
2_4
36a
37a
24a
25a
26a
27a
28a
16
18
19
34
35
1
L
CARTE A MICROCIRCUIT
LECTEUR DE CARTE
ORDINATEUR PERSONNEL
PIN OK ?
Nn
Kn
A
Kn+1 = f(Kn, Nn+1)
Nn+1
PIN
CLAVIER
T
PRODUCTION CHALLENGE (64 bits)
FORMATAGE ET AFFICHAGE
+ 1
8
9
10
13
20
21
22
23
24
25
26
27
28
32
33
36
37

FIG. 2

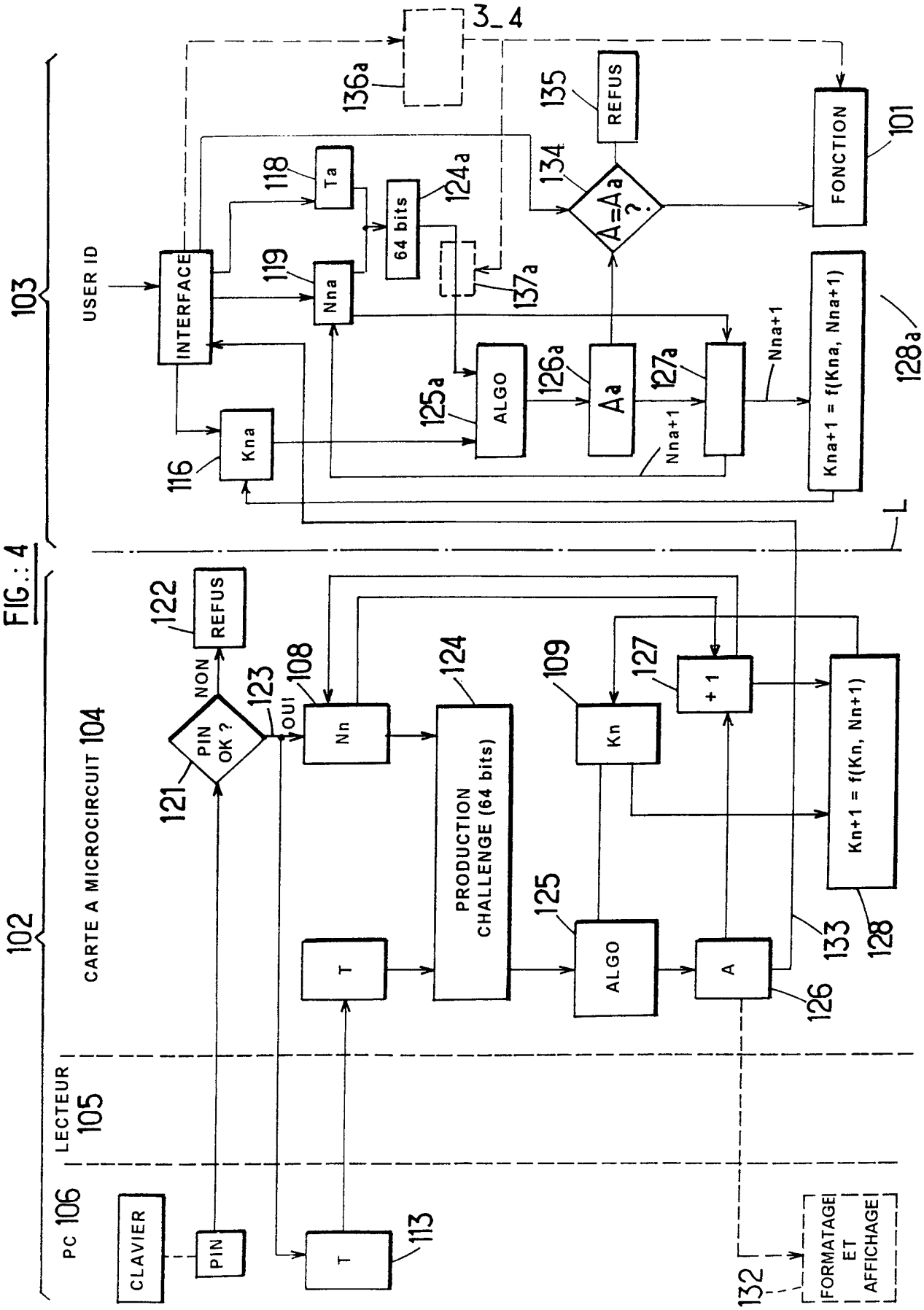

3_4
136a
135
REFUS
FONCTION
101
118
Ta
124a
64 bits
134
A=Aa ?
USER ID
INTERFACE
119
Nna
137a
103
125a
ALGO
126a
Aa
127a
Nna+1
Kna+1 = f(Kna, Nna+1)
128a
116
Kna
L
122
REFUS
NON
123
OUI
108
124
109
127
+ 1
121
PIN OK ?
Nn
PRODUCTION CHALLENGE (64 bits)
Kn
Kn+1 = f(Kn, Nn+1)
CARTE A MICROCIRCUIT 104
102
T
125
ALGO
A
133
128
126
LECTEUR 105
PC 106
CLAVIER
PIN
T
113
132
FORMATAGE ET AFFICHAGE

FIG.: 4

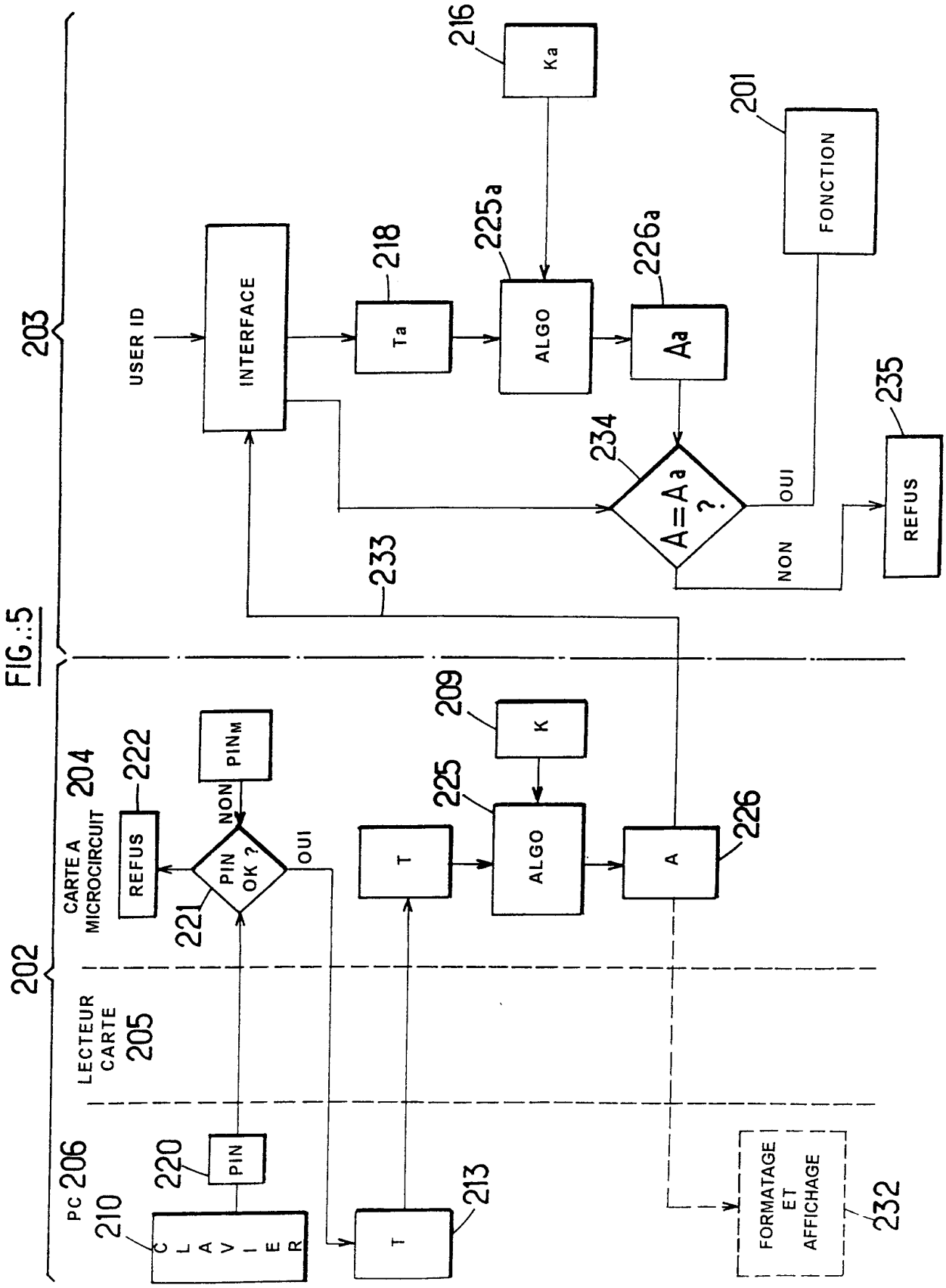

203
USER ID
INTERFACE
Ta
218
ALGO
225a
Aa
226a
Ka
216
FONCTION
201
A=Aa ?
234
OUI
NON
REFUS
235
233
202
CARTE A MICROCIRCUIT 204
LECTEUR CARTE 205
PC 206
PIN OK ?
221
NON
OUI
REFUS
222
PINM
T
ALGO
225
K
209
A
226
PIN
220
CLAVIER
210
T
213
FORMATAGE ET AFFICHAGE
232

FIG.:5

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/FR 98/02104

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,Y A	WO 97 36264 A (ACTIVCARD) 2 October 1997 see page 7, line 28 - page 22, line 2 see figure 2	1-4 5-10
Y A	US 4 974 193 A (BEUTELSPACHER ALBRECHT ET AL) 27 November 1990 see the whole document	1-4 11,13
A	DE 42 23 258 A (TELEFUNKEN MICROELECTRON) 20 January 1994 see the whole document	1-4

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 February 1999	25/02/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bocage, S

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/FR 98/02104

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9736264 A	02-10-1997	FR 2747815 A	24-10-1997
		US 5802176 A	01-09-1998
		AU 2297597 A	17-10-1997
		EP 0891611 A	20-01-1999
US 4974193 A	27-11-1990	DE 3706955 A	15-09-1988
		DE 3889481 D	16-06-1994
		EP 0281057 A	07-09-1988
		ES 2051780 T	01-07-1994
		JP 63228353 A	22-09-1988
DE 4223258 A	20-01-1994	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

De[illegible]de Internationale No
PCT/FR 98/02104

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
P,Y A	WO 97 36264 A (ACTIVCARD) 2 octobre 1997 voir page 7, ligne 28 - page 22, ligne 2 voir figure 2	1-4 5-10
Y A	US 4 974 193 A (BEUTELSPACHER ALBRECHT ET AL) 27 novembre 1990 voir le document en entier	1-4 11,13
A	DE 42 23 258 A (TELEFUNKEN MICROELECTRON) 20 janvier 1994 voir le document en entier	1-4

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
17 février 1999	25/02/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bocage, S

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

De de internationale No
PCT/FR 98/02104

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9736264 A	02-10-1997	FR 2747815 A	24-10-1997
		US 5802176 A	01-09-1998
		AU 2297597 A	17-10-1997
		EP 0891611 A	20-01-1999
US 4974193 A	27-11-1990	DE 3706955 A	15-09-1988
		DE 3889481 D	16-06-1994
		EP 0281057 A	07-09-1988
		ES 2051780 T	01-07-1994
		JP 63228353 A	22-09-1988
DE 4223258 A	20-01-1994	AUCUN	